UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America, Plaintiff, v. Drayton Dean Wilson, Defendants.	Case No. 21-cr-222 WMW/ECW **REPORT AND RECOMMENDATION**

This matter is before the Court on Defendant Drayton Dean Wilson's Motion to Suppress Evidence Obtained as a Result of Search and Seizure (Dkt. 30).

This case has been referred to the undersigned United States Magistrate Judge for a report and recommendation pursuant to 28 U.S.C. § 636 and Local Rule 72.1. The parties agreed to have the Motion decided by the Court on the pleadings with no hearing. (Dkts. 33, 34.)

I. INTRODUCTION

Defendant Drayton Dean Wilson is charged by Indictment with one count of Receipt of Child Pornography and two counts of Possession of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(2), (a)(4), 2252(b)(1), and (b)(2). (Dkt. 1.) Wilson filed a motion to suppress evidence obtained pursuant to the execution of five search warrants. As set forth above, the parties have agreed the search warrants and underlying applications and affidavits, Government Exhibits 1-5, could be submitted to this Court for a four-corners review.

II. FACTUAL BACKGROUND

A. May 28, 2020, Federal Search and Seizure Warrant, Application, and Affidavit for Information Associated with E-Mail Address DEANW3876@gmail.com, Stored at Google, LLC (Gov't Ex. 1)

On May 18, 2020, Special Agent Robert Blackmore ("SA Blackmore") with the Federal Bureau of Investigation applied for a search warrant for the search of information stored in the servers that are associated with the e-mail address DEANW3876@ gmail.com, which was stored at a premises controlled by Google LLC ("Google"). (Gov't Ex. 1.)

In his supporting affidavit, SA Blackmore claimed that there was probable cause to believe that the email address DEANW3876@gmail.com ("DEANW3876 Account") was used to receive, possess, distribute, and transport child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. (*Id.* ¶ 3.) SA Blackmore asserted, based on his training and experience, that he has learned that Google provides a variety of on-line services, including electronic mail ("e-mail" or "Gmail") access, to the general public. (*Id.* ¶ 8.) Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, such as the DEANW3876 Account, and subscribers obtain an account by registering with Google, during which Google asks subscribers to provide basic personal information. (*Id.*) As such, SA Blackmore asserted that the servers and computers of Google were likely to contain stored electronic communications and information concerning subscribers (such as subscriber's full name, physical address, telephone numbers and other identifiers, and alternative e-mail addresses) and their use of Google services, which may constitute evidence of the crimes under investigation. (*Id.* ¶¶ 8-10.) In

addition, SA Blackmore claimed, based on his training and experience, that e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. (*Id.* ¶ 11.). SA Blackmore also represented, based on his training and experience, that e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. (*Id.*) Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access an e-mail account. (*Id.*)

Further, SA Blackmore provided information regarding the National Center for Missing and Exploited Children ("NCMEC"), the leading nonprofit organization in the United States working with law enforcement, families, and the professionals who serve them on issues related to missing and sexually exploited children. (*Id.* ¶ 13.) Pursuant to a congressional mandate, NCMEC launched its CyberTipline in 1998, which provides online users an effective means of reporting Internet-related child sexual exploitation. (*Id.*) Federal law mandates that all electronic communication service or remote computer service providers report all facts or circumstances from which there is an apparent violation of federal child pornography laws to the CyberTipline. (*Id.* (citing 18 U.S.C. § 2258A).)

SA Blackmore also provided the following evidence regarding the DEANW3876 Account:

- On or about March 19, 2020, SA Blackmore was contacted by Sergeant Jim Andersen ("Sergeant Andersen") of the St. Paul Police Department regarding a child pornography investigation involving Wilson, a registered predatory sex offender in

Minnesota, who has two prior sexual contact offenses against minors (prior to when Wilson had turned 18 years old), involving a 2016 conviction related to a four-year-old victim and 2009 conviction related to a two-year-old victim. (*Id.* ¶ 15.)

- Sergeant Anderson provided information to SA Blackmore showing that on or about January 5, 2020, the NCMEC received a report from Google, advising that it had found what it believed to be two files depicting child pornography content stored in Google's Gmail infrastructure, and that Google reported that the account involved with this content was the verified email address DEANW3876@gmail.com. Google further provided numerous IP addresses from which the DEANW3876 Account was accessed. (*Id.* ¶ 16.)

- Google believed this content to be child pornography based on hash value matches to images they had previously viewed. (*Id.* ¶ 17.)

- Based on SA Blackmore's training and experience, he knew that a hash value is a unique identifier for a file, sometimes described as the file's fingerprint or DNA. (*Id.*) It is generated through the use of a hash function (a mathematical algorithm), and can be represented by an alphanumeric string of characters. (*Id.*) Any change, however small, to the contents of a file will change that file's hash value. Because the file name is not hashed, a change to a file's name does not change the hash value of the file itself. (*Id.*) The hash value used in this case was MD5. (*Id.*) Multiple hash functions can be used to identify a file, including MD5. (*Id.*) Because it is possible for two different files to possess the same hash value, the MD5 algorithm has been found to be insufficient for cryptographic use, however the odds of two random files (much less two functioning video files) possessing the same MD5 hash value have been calculated to be in excess of 1 in 2 quintillion. (*Id.*)

- The images in this case were not directly viewed by Google or NCMEC, as their hash values matched files that had been previously viewed. (*Id.* ¶ 18.) In the report submitted to NCMEC, Google advised that historically a person had reviewed a file whose hash value matched the hash value of the reported image and determined it contained apparent child pornography. (*Id.*)

- The NCMEC used this information to generate CyberTipline Report #62382143. (*Id.*) This report was then sent on an unspecified date to the Minnesota Bureau of Criminal Apprehension/Internet Crimes Against Children Task Force (hereinafter "BCA") for further investigation. (*Id.*)

- The BCA subpoenaed Google for information related to the DEANW3876 Account. Google reported that the DEANW3876 Account was subscribed to a Dean Wilson, that the account was created on December 15, 2019, and was associated with

telephone number 612-261-97XX. (*Id.* ¶ 20.) Logs showed that the majority of IP addresses used to access this account were registered to T-Mobile. (*Id.*)

- The BCA subpoenaed T-Mobile/MetroPCS for information related to telephone number 612-261-97XX and the IP addresses used to access the DEANW3876 Account. (*Id.* ¶ 21.) Records provided in response to these subpoenas showed that the IP addresses were accessed by phone number 612-261-97XX and that this phone number is subscribed to a person in the name of Dean Wilson, XXX Magnolia Avenue East, St Paul, Minnesota. (*Id.*) The number was active at the time of the application, with an effective date of December 14, 2019. (*Id.*)

- Wilson was on probation under the supervision of the Minnesota Department of Corrections (hereinafter "MNDOC") and MNDOC records showed that Wilson's listed telephone number, as of February 6, 2020, was (612) 261-97XX. (*Id.* ¶¶ 22-23.)

- Wilson's MNDOC records showed several instances of probation violations and non-compliance with the sex offender registration requirements, including the purchase/possession of sexually explicit materials, as well as possession and use of an internet capable device. (*Id.* ¶ 24.)

On May 18, 2020, the Honorable David T. Schultz, United States Magistrate Judge, issued the search warrant, which authorized the search for and seizure of information from Google, including, but not limited to, information: pertaining to sending or receiving child pornography; evidence indicating how and when the Gmail account was accessed to determine the geographic and chronological context of the account relating to the crime under investigation; evidence related to the Gmail account owner's state of mind and knowledge as it relates to the crime under investigation; the identity of the person who created, used, or communicated with the Gmail account; and evidence of production, possession, or export of images depicting victims of the crimes. (Gov't Ex. 1, attachs. A and B.)

B. May 29, 2020, Federal Search and Seizure Warrant, Application, and Affidavit issued for Information Associated with E-Mail Address DW3876@gmail.com, Stored at Google, LLC (Gov't Ex. 2)

On May 29, 2020, SA Blackmore also applied for a search warrant for the search and seizure of information stored in the servers that are associated with the e-mail address DW3876@gmail.com ("DW3876 Account"), which was stored at premises controlled by Google. (Gov't Ex. 2.)

SA Blackmore's supporting affidavit provided similar information contained in Government Exhibit 1 regarding Google e-mail accounts and the NCMEC. (*Id.* ¶¶ 8-13, 16-17.)

The Affidavit also contained similar information contained in Government Exhibit 1 regarding Wilson's background, the DEANW3876 Account, the fact that Google had communicated to the NCMEC that the DEANW3876 Account contained files with a same hash value as files containing child pornography, and the information subpoenaed by the BCA from Goggle as to the DEANW3876 Account. (Gov't Ex. 2 ¶¶ 18-27.)

In addition, the Affidavit provided additional information learned from issuance of the initial search warrant at Government Exhibit 1 related to the DEANW3876 Account:

- Google provided responsive materials showing that the e-mail address DEANW3876 Account is subscribed to a person in the name of Dean Wilson with telephone number 612-261-97XX.

- Google also provided the two files that they submitted to the NCMEC, both of which were discovered to contained depictions of minors engaged in sexual acts.

- In addition, Google provided email content for the DEANW3876 Account. A review of emails in this account showed that on January 4, 2020, the DEANW3876 Account sent an email to the subject DW3876 Account. The file titled XXXXXX-

hgt.gif, described above as one of the files containing depictions of minors engaged in sexual acts, was attached to this email.

- Due to the similarity in the names of the DEANW3876 and DW3876 Gmail Accounts, SA Blackmore believed it was possible that Wilson used an alternate email account to send this email, with its attachment, to himself.

(*Id.* ¶¶ 28-31.)

On May 29, 2020, the Honorable Becky R. Thorson, United States Magistrate Judge, issued the search warrant. The search warrant authorized the seizure of information from Google, including, but not limited to information: pertaining to sending or receiving child pornography; communications regarding child pornography; any indicia of child pornography; evidence indicating how and when the Gmail account was accessed to determine the geographic and chronological context of the account relating to the crime under investigation; evidence related to the Gmail account owner's state of mind and knowledge as it relates to the crime under investigation; the identity of the person who created, used, or communicated with the Gmail account; and evidence of production, possession, or export of images depicting victims of the crimes. (Gov't Ex. 2, attachs. A and B.)

C. September 27, 2020, State (Dakota County) Search and Seizure Warrant, Application, and Affidavit Issued for Wilson's Person, Vehicle (Pontiac Grand AM, MN 821-XXX), and Residence (XX Orme St. E, Apt XXX, West St. Paul) (Gov't Ex. 3)

On September 27, 2020, Special Agent Lucas Munkelwitz ("SA Munkelwitz") with the BCA sought a search warrant for Wilson's person; a Pontiac Grand AM, MN 821-XXX; and a residence located at XX Orme St. E, Apt XXX, West St. Paul, Minnesota ("Orme Street Residence"). In support of the search warrant, SA Munkelwitz

provided the following information relating to his training and experience with respect to computer technology, child pornography, and those who collect child pornography:

- Individuals who produce or collect child pornography can distribute the produced/collected images/videos quickly and easily using a computer/smartphone and a standard Internet connection. Electronic contact can be made to millions of computers around the world. Child pornography files can be transferred via email or through file transfer protocols to anyone with access to a computer or smartphone with internet connection.

- The computer or other electronic device's capability to store images in digital form makes it an ideal repository for child pornography. Images can be stored internally in a home computer on its "hard drive" or externally on disks or other removable media storage device.

- Large amounts of data can be stored on mobile telephones and data storage devices no larger than a credit card. It is common for individuals to keep devices like mobile telephones and data storage devices in their vehicles and on their persons due to their relatively small size and mobility. In addition, computers, tablets, and other larger devices can be stored easily in a vehicle or in a briefcase or bag carried by a person.

- It is common for individuals who collect child pornography to retain their material for lengthy periods of time. These individuals value their sexually explicit materials highly and will rarely voluntarily dispose of or part with their materials. In addition to the emotional value/psychological support the images/videos have to the collector, the images/videos are intrinsically valuable for trading and/or selling. Therefore, these items are rarely if ever destroyed or deleted.

- Further, even if a collector deletes his collection, "artifacts" or "remnants" of the collection can remain on the collector's electronics until written over.

- Individuals who have a sexual interest in children or who collect images of children will go to great lengths to conceal and protect their materials from discovery, theft, and damage. They often maintain their collections in a safe, secure and private environment such as within a laptop computer, cell phone, or USB device. In your affiant's experience, collectors maintain their collections on items stored in the privacy and security of their home or vehicle.

- Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period.

(Gov't Ex. 3 at 3-5.) SA Munkelwitz also provided information similar to SA Blackmore, *supra*, regarding the CyberTipline operated by the NCMEC. (*Id.* at 8.)

With respect to the specific facts involving Wilson and the places to be searched, SA Munkelwitz provided in relevant part as follows:

- A January 5, 2020 CyberTipline report received from Google reported a Dean Wilson with mobile phone 612-261-97XX, and DEANW3876@gmail.com, had stored two files within the Google Gmail infrastructure with hash values of known images of child exploitation materials.

- A February 19, 2020 CyberTipline report received from Microsoft reported having viewed three images from a Microsoft OneDrive (Cloud Storage) account that it verified appeared to be sexually explicit images involving minor children. A subpoena to Microsoft revealed that the user of the account was a Dean Wilson with an alias name of 161226197XX, and an email address of DEANW3876@gmail.com. The IP address at issue belonged to a T-Mobile account and the recovery number was 612-261-97XX.

- A subpoena to T-Mobile for the IP address revealed that the account belonged to a Dean Wilson, at XXX Magnolia Ave, E, Saint Paul. According to SA Munkelwitz, XXX Magnolia Avenue is the address for Restoration Counseling and Community Services, which is a treatment facility that predatory offenders attend. The home number for the account was 612-274-56XX.

- SA Munkelwitz found that Level 2 Minnesota Predator, Drayton Dean Wilson had registered the phone number 612-261-97XX with the BCA Predatory Offenders Registration Unit from February 6, 2020, through the date of the affidavit, and that his registered address was Green House Recovery Center, XXX Greenbrier in Saint Paul, and that he had previously been at the XXX Magnolia Ave, E Green House Recovery Center.

- In 2012, Wilson was sentenced to 36 months for Second Degree Criminal Sexual Conduct involving a victim under the age of 13. In 2014, Wilson was found to have violated his parole by having an unauthorized cell phone and unauthorized possession of sexually explicit materials and was recommitted back to prison for this violation. Wilson was released from prison on November 27, 2019 and at the time of the Affidavit was under the supervision of the MNDOC.

- On September 24, 2020, SA Munkelwitz attempted to execute a search warrant at Green House Recovery Center and staff there shared that Wilson had not been at the Center for at least two months.

- Wilson's parole agent told SA Munkelwitz that Wilson's new address was XXX Freemont Avenue, St. Paul, Minnesota. Wilson had contacted her using a 651-350-62XX number, as recently as September 24, 2020, and told the parole agent on this date that he had obtained a new vehicle with Minnesota License Plate 821 XXX, and told her that he was about to get a job and would get picked up for work at XXX Greenbrier Street, St. Paul, Minnesota 55106.

- On 9/24/2020, SA Munkelwitz reviewed Wilson's state identification and became aware that Wilson listed the address XXX Greenbrier Street, St. Paul, MN 55106, as his address for his new driver's license.

- SA Munkelwitz obtained a GPS tracking warrant for the 651-350-62XX number, which showed the phone location appeared to be in the area of Orme Street Residence and GPS locations stayed consistently at this location into September 25, 2020.

- Officer surveillance of Wilson, continued GPS tracking for the 651-350-62XX number, the location of the Wilson's vehicle, and Facebook postings also supported that Wilson was staying at the Orme Street Residence.

(Gov't Ex. 3 at 9-15.)

On September 27, 2020, Dakota County Minnesota State District Judge Tanya O'Brien, issued the search warrant for Wilson's person, the Orme Residence, and Wilson's Pontiac Grand Am. The search warrant authorized the seizure of a number items, including, but not limited to: computers, hard drives, media in whatever form, personal electronic devices, data contained in hard drives or removable media (including deleted electronic information) related to child pornography, papers and effects showing the possession or distribution as well as enticement of children online, proof of residency, camera and video equipment that may be used for child pornography, depictions of

minors engaged in actual or simulated sexual acts; and depictions of nudity involving minors. (Gov't Ex. 3 at 19-20.)

D. October 15, 2020, Federal Search and Seizure Warrant, Application, and Affidavit Issued for Information Associated with User ID 34001206AB386; Sign In Name DEANW3876@gmail.com; and Alias Name 161226197XX, Stored at Microsoft Corporation (Gov't Ex. 4)

On October 15, 2020, SA Blackmore sought a search warrant for the Microsoft OneDrive account associated with ESP USER ID: 34001206AB386, sign in name DEANW3876@ GMAIL.COM, and Alias Name 161226197XX. (Gov't Ex. 4.)

The supporting affidavit included that Microsoft OneDrive is a cloud storage service that allows users to store personal files, including photographs, in one place, share those files with others, and access those files from any device connected to the Internet. (*Id.* ¶¶ 9-11.) The service offers five gigabytes of free personal storage and additional personal storage can be purchased by the user. (*Id.* ¶ 11.) In general, users obtain accounts by registering on a Microsoft Corporation and Microsoft may collect certain information such as the user's name, telephone number, physical addresses, and email addresses. (*Id.* ¶ 12.)

Similar to the search warrants at Government Exhibits 1 and 2, SA Blackmore also provided a general background regarding NCMEC and its CyberTipline, as well as background regarding Wilson as a registered predatory sex offender in Minnesota. (*Id.* ¶¶ 19-21.) In addition, the affidavit also contained similar information found in Government Exhibit 1 regarding Wilson; the DEANW3876 Account; the fact that Google had communicated to the NCMEC that the DEANW3876 Account contained files with

the same hash values as files containing child pornography; and the information subpoenaed by the BCA from Goggle as to the DEANW3876 Account, including that it was associated with the 612-261-97XX number subscribed to a Dean Wilson. (Gov't Ex. 4 ¶¶ 22-27.) MNDOC records listed Wilson's telephone number as 612-261-97XX. (*Id.* ¶ 29.)

The supporting affidavit also provided that as result of Magistrate Judge Schultz's May 18, 2020 Search Warrant, Google provided information that the email address of DEANW3876 was subscribed in the name of Dean Wilson with a telephone number of 612-261-97XX. (*Id.* ¶ 32.) In addition, Google provided the two files they had submitted to the NCMEC as the basis of the CyberTipline report, which according to SA Blackmore contained images of minors in sexual acts. (*Id.* ¶ 32.) Further, Google provided information that the DEANW3876 Account sent one of the images on January 4, 2020 to the DW3876 Account. (*Id.* ¶ 33.)

Given this information, the affidavit also represented that SA Blackmore sought a search warrant from Google regarding the DW3876 Account, which was issued by Magistrate Judge Thorson and served upon Google on June 1, 2020. (*Id.* ¶ 34.) In response to the search warrant signed by Judge Thorson, Google provided responsive materials showing that the DW3876 Account was subscribed to an individual named Dean Landers with telephone number 612-261-97XX, which was the number Wilson had provided to MNDOC as his phone number. (*Id.* ¶ 35.) Responsive materials provided by Google contained images and videos uploaded to Google Photos, which included numerous images and videos depicting sexual acts with minors, photographs of Wilson, a

picture of his Minnesota driver's license, and a picture of a check made out to Wilson. (*Id.* ¶ 36.)

On or about February 19, 2020, the NCMEC received a report from Microsoft, advising that they had found what they believed to be three files depicting sexual acts with minors to have been uploaded to the subject Microsoft OneDrive account on February 18, 2020. One of these files was reviewed by Microsoft and SA Blackmore, which he claimed based on his experience and training depicted a minor prepubescent child in a sexual act with an adult. (*Id.* ¶¶ 38-39.) In response to a BCA subpoena, Microsoft provided that the account was registered in Wilson's name, that the sign-in was DEANW3876@GMAIL.COM, and the alias name for the account was 1-612-261-97XX. (*Id.* ¶ 40.) A subpoena to Google showed that the DEANW3876@GMAIL.COM was registered in Wilson's name, with the recovery number of 612-261-97XX, and that a device with a T-Mobile IP address had attempted to access the e-mail account on March 9, 2020 and May 3, 2020, which according to T-Mobile (via a separate BCA subpoena) were two cell phones registered in Wilson's name. (*Id.* ¶¶ 41-42.)

During the execution of a September 28, 2020 search warrant of the Orme Street Residence, SA Blackmore and SA Munkelwitz conducted a Mirandized interview of Wilson, who acknowledged not being compliant with the predatory offender registration requirements, acknowledged using the DEANW3876 and DW3876 Accounts, and also acknowledged using his previous cell phone to view child pornography that he received from another person in an Internet chat room. (*Id.* ¶¶ 43-44.) He did not acknowledge

using the e-mail accounts to view, receive, distribute or possess child pornography. (*Id.* ¶ 44.)

On October 15, 2020, United States Magistrate Judge Hildy Bowbeer issued the search warrant for the Microsoft OneDrive Account. (Gov't Ex. 4 at 1.) The search warrant authorized the seizure of information from Microsoft, including, but not limited to information: pertaining to sending or receiving child pornography; communications regarding child pornography; any indicia of child pornography; evidence indicating how and when the account was accessed in order to determine the geographic and chronological context of the account relating to the crime under investigation; evidence related to the account owner's state of mind and knowledge as it relates to the crime under investigation; the identity of the person who created, used, or communicated with the account; and evidence of production, possession, or export of images depicting victims of the crimes. (Gov't Ex. 4 at 24-26.)

E. November 3, 2021 Search Warrant for Facebook Account

On November 3, 2021, SA Blackmore sought a search warrant requiring Facebook to disclose to the government records and other information in its possession associated with Facebook user ID 100045976296956 and Facebook username DEAN.LANDERS.3304. (Gov't Ex. 5.) In particular, the Search Warrant sought to seize information related to sexual contact with minors; images of child pornography; information and records related to the production, possession, receipt or distribution of child pornography; content of messages, chats or communications relating to the sexual exploitation of children; evidence as to who used or owned the Facebook account;

evidence as to how the account was accessed; evidence related to the user's state of mind; and evidence regarding the use of the contents of the DEANW3876@GMAIL.COM and DW3876@GMAIL.COM accounts. (*Id.* at 30.)

In addition to the information provided in support of probable cause for the search warrants at Government Exhibits 1, 2, and 4, SA Blackmore provided the following additional relevant information in his supporting Affidavit:

> On October 19, 2021, Wilson was indicted by a Grand Jury in the District of Minnesota on one count of Receipt of Child Pornography, in violation of Title 18, U.S.C., Section 2252(a)(2), and two counts of Possession of Child Pornography, in violation of Title 18, U.S.C., Section 2252(a)(4)(b).
>
> As part of preparing to arrest WILSON I contacted his parole officer to obtain updated address and contact information. The parole officer advised that she had recently been contacted by WILSON's ex-girlfriend who provided a screenshot of the SUBJECT ACCOUNT, which contains a profile picture of WILSON. The ex-girlfriend stated that she was not aware that he could not have Facebook. She further stated that WILSON now lived in the same town as her nieces and that she was terrified that she [sic] would show up at her house.

(Gov't Ex. 5 ¶¶ 52-53.)

SA Blackmore also represented that in his experience and training, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook can indicate who has used or controlled the Facebook account; can show how and when the account was accessed or used, including the IP addresses from which users access their accounts along with the time and date, the location of the user; and may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. (*Id.* ¶ 25.)

On November 3, 2021, Magistrate Judge Thorson issued the search warrant for the subject Facebook Account.

III. ANALYSIS

A. Evidence Discovered During the Search of Gmail Accounts, Microsoft One Drive Account, and Facebook Account (Gov't Exs. 1, 2, 4, and 5)

Wilson argues that the search warrants obtained as to the two Gmail accounts (Gov't Exs. 1 and 2); the Microsoft OneDrive account (Gov't Ex. 4); and the Facebook account (Gov't Ex. 5) all lacked probable cause because they were issued based on information that was stale by the time the respective search warrants were issued. (Dkt. 30 at 3; Dkt. 36 at 3.) In particular, Wilson contends that each of these warrants were applied for and issued several months after Google and Microsoft reported finding a number of images allegedly containing child pornography on Wilson's alleged accounts. (Dkt. 36 at 5.) While Wilson concedes that normally a lapse of time would not be a problem with the alleged crime of child pornography, he argues:

> Staleness for purposes of assessing probable cause, however, is not merely a question of time. The quality of staleness from a probable cause perspective also includes other individual features in the affidavit supporting grounds to search. Such features are lacking here. This is not a case where the affidavit recounted various incidents or uploading, viewing or possession other images other than small number of the images reported on January 4, 2021 (Government Exhibit 1), and February 19, 2021 (Government Exhibit 4), and the email sent on January 4, 2021 (Government Exhibit 3). The search warrant application in this case failed to demonstrate behavior indicative of a preferential collector or that Mr. Wilson was even a collector. As a result, all three of the above search warrants were stale.

(*Id.* at 5-6.)

The Government counters that the Eighth Circuit has consistently held that evidence developed within several months of an application for a search warrant for a child pornography collection and related evidence is not stale, that staleness with respect to child pornography is considered differently than evidence in narcotic crimes as it relates to staleness, and that Wilson's argument ignores the facts in search warrants evidencing his history as a sexual predator.[1] (Dkt. 37 at 9-11.)

Ordinarily, searches pursuant to a warrant are reviewed to determine if there was probable cause for the search in the search warrant application and affidavit. *See Illinois v. Gates*, 462 U.S. 213, 236 (1983). "Probable cause exists when, given the totality of the circumstances, a reasonable person could believe there is a fair probability that contraband or evidence of a crime would be found in a particular place." *United States v. Fladten*, 230 F.3d 1083, 1085 (8th Cir. 2000) (citing *Gates*, 462 U.S. at 238). The task of a court issuing a search warrant is "simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. "Probable cause is a fluid concept that focuses on 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" *United States v. Colbert*, 605 F.3d 573, 576 (8th Cir. 2010)

[1] The Court notes that the Government argues in the alternative, that even if any of the search warrants lacked sufficient probable cause, all of the search warrants fall under the *Leon* exception (Dkt. 37 at 14-15), which the Court addresses *infra.*

(quoting *Gates*, 462 U.S. at 231). In reviewing the decision of the issuing court, the duty of the reviewing court is simply to ensure that the court had a substantial basis for concluding that probable cause existed. *See Gates*, 462 U.S. at 238-39 (citation omitted); *see also United States v. LaMorie*, 100 F.3d 547, 552 (8th Cir. 1996) (citation omitted) ("Our duty as a reviewing court is to ensure that the issuing judge had a 'substantial basis' for concluding that probable cause existed, and we owe substantial deference to the determination of probable cause by the issuing judge."). As to what this Court should consider when reviewing a search warrant for probable cause, "[w]hen the [issuing judge] relied solely on the affidavit presented to him, 'only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause.'" *United States v. Solomon*, 432 F.3d 824, 827 (8th Cir. 2005) (citing *United States v. Etheridge*, 165 F.3d 655, 656 (8th Cir. 1999), quoting *United States v. Gladney*, 48 F.3d 309, 312 (8th Cir. 1995)); *United States v. Smith*, 581 F.3d 692, 694 (8th Cir. 2009) (quoting *United States v. Reivich*, 793 F.2d 957, 959 (8th Cir. 1986)).

"A warrant becomes stale if the information supporting the warrant is not sufficiently close in time to the issuance of the warrant and the subsequent search conducted so that probable cause can be said to exist as of the time of the search." *United States v. C-Cervantes*, 868 F.3d 695, 700 (8th Cir. 2017) (cleaned up). "[T]here is no bright-line test for determining when information is stale." *United States v. Gettel*, 474 F.3d 1081, 1086 (8th Cir. 2007) (cleaned up). "The passage of time is not necessarily the controlling factor in determining staleness, as other factors, such as the nature of the criminal activity involved and the kind of property subject to the search,

must be considered." *Id.* (cleaned up); *see also United States v. Augard*, 954 F.3d 1090, 1094 (8th Cir. 2020), *cert. denied*, 141 S. Ct. 1397 (2021) ("While there is no bright-line test for determining staleness, we look to a variety of factors, including the nature of the criminal activity and the type of property subject to search.").

Here, the Google Gmail search warrants (Gov't Exs. 1-2) were initially predicated by the CyberTipline report by Google to NCMEC[2] on January 5, 2020 that there were two child pornography files associated with Wilson's DEANW3876@gmail.com email account. SA Blackmore applied for and received the initial Search Warrant for this account on May 18, 2020. The second search warrant to Google for the DW3876 Account, also initially based on the January 5, 2020 report, was obtained on May 29, 2020.

Similarly, the CyberTipline report by Microsoft to NCMEC on February 19, 2020 communicated that three files, depicting sexual acts with minors, were uploaded to the subject Microsoft OneDrive account on February 18, 2020, and SA Blackmore did not seek a search warrant until October 15, 2020.

With respect to determining when information is stale or the probative value of all suspected child pornography activities, the Eighth Circuit has recognized "the compulsive nature of the crime of possession of child pornography and the well-established hoarding habits of child pornography collectors[.]" *United States v. Notman*,

---

[2] The Court notes that Google's and the NCMEC's actions do not amount to a search by a governmental agent for the purposes of the Fourth Amendment. *See United States v. Ringland*, 966 F.3d 731, 736-37 (8th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021).

831 F.3d 1084, 1088 (8th Cir. 2016). Given its compulsive nature and established hoarding, the crime of possessing child pornography is unique with respect to the issue of whether supporting information is stale. *See United States v. Manning*, 361 F. Supp. 3d 839, 845-46 (D. Minn. 2019), *aff'd*, 833 F. App'x 43 (8th Cir. 2021). Moreover, "'[s]taleness' is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file," as this is "not the type of evidence that rapidly dissipates or degrades." *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012); *compare United States v. Kennedy*, 427 F.3d 1136, 1142 (8th Cir. 2005) ("[I]nformation of an unknown and undetermined vintage relaying the location of mobile, easily concealed, readily consumable, and highly incriminating narcotics could quickly go stale in the absence of information indicating an ongoing and continuing narcotics operation."). As such, even though only a few files of child pornography were reported in the affidavits at issue, the small number of files does not make the information stale given the nature of the crime and the nature of the electronic evidence.

In addition, as to the Google Gmail search warrants,[3] five and half months passed from the Google's notification of child pornography and issuance of the search warrants. Courts in the Eighth Circuit have consistently held that search warrants issued five months or more after discovering information linking a place to child pornography are valid, and information they rely upon is not stale for Fourth Amendment purposes. *See*,

[3] The Court addresses the May 18 and 29 Google Gmail search warrants together since the discovery of the DW3876 Account was the result of the execution of the search warrant for the DEANW3876 Account.

e.g., *United States v. Lemon*, 590 F.3d 612, 615 (8th Cir. 2010) (concluding that eighteen-month-old evidence of possession of child pornography is not stale as a matter of law, given that "technological advances have increased the ease with which child pornography may be produced, maintained, or distributed-making it all the more likely that the contraband will be retained"); *United States v. Estey*, 595 F.3d 836, 840 (8th Cir. 2010) (holding a search warrant issued five months after discovering information linking the defendant's residence with child pornography was valid; "evidence developed within several months of an application for a search warrant for a child pornography collection and related evidence is not stale") (collecting cases); *United States v. Koelling*, 992 F.2d 817, 823 (8th Cir. 1993) (referring to *United States v. Rabe*, 848 F.2d 994, 997 (9th Cir. 1988)), which found in part based on expert opinion that pedophiles collect materials for years and based in part on knowledge of the defendant's receipt of child pornography in 1984, a search warrant issued in 1986 was not premised on stale information); *Manning*, 361 F. Supp. 3d at 845-46 (five months or longer). As such, the Court finds that the search warrants at Government Exhibits 1 and 2 are not based on stale evidence in light of the offense, the nature of the evidence, and the length of time between the discovery of the evidence and the issuance of the search warrants—in this case between 5 and 6 months. Further support for this finding is the fact that the affidavits for these search warrants also included that Wilson is a registered sex offender arising out of sexual offense conviction against four-year-old and two-year old victims. In sum, the totality of this information provided the Magistrate Judges with a sufficient probable cause to believe that Wilson was engaged in the possession of child pornography using the subject

Google email accounts[4] as of the date of the May 18, 2020 and May 29, 2020 search warrants.[5]

The result is no different for the October 15, 2020 search warrant for the Microsoft OneDrive account stemming from the February 19, 2020 CyberTipline report by Microsoft to NCMEC communicating that three files depicting sexual acts with minors were uploaded to the subject Microsoft OneDrive account on February 18, 2020. While the issuance of the search warrant occurred approximately eight months after the Microsoft report, for the same reasons as set forth above with respect to the Google email accounts, the Court finds that evidence relied upon, information regarding the three images, is not stale. Moreover, the supporting affidavit contained the information that the May 18, 2020 and May 29, 2020 search warrants resulted in the seizure of numerous images and videos depicting sexual acts with minors, photographs of Wilson, and a picture of his Minnesota driver's license. In other words, just four and a half months earlier there was evidence that Wilson was storing child pornography on the cloud. This, coupled with information in the affidavit of Wilson's September 28, 2020 Mirandized

---

[4] Wilson does not dispute that he used the subject Google email accounts, as claimed in the search warrants affidavits. Indeed. the affidavits sufficiently connect the email accounts listing the 612-261-97XX number to the same phone number listed for Wilson by the MNDOC.

[5] The Court notes that probable cause for the May 29, 2020 search warrant for the DW3876 Account is further supported by the discovery and review of images of child pornography on the account DEANW3876 Account as part of the execution of the May 20 Search warrant, one of which was sent from the DEANW3876 Account to the DW3876 Account owned by Wilson.

statement that he used his previous cell phone to view child pornography that he received from another person in an Internet chat room, leads to the conclusion that the supporting evidence for the October 15, 2020 search warrant for the Microsoft OneDrive account was not stale and that based on the totality of circumstances, the October 15, 2020 search warrant is supported by sufficient probable cause that child pornography would be found in connection with Wilson's Microsoft OneDrive account.

Similarly, the Court finds for the same reasons that the November 3, 2021 Facebook search warrant, which is based on the above evidence, and the information regarding the October 19, 2021 Grand Jury Indictment of Wilson related to receipt and possession of child pornography, is not based on stale evidence.

In sum, the Court finds that Wilson's Motion to Suppress as to the search warrants at Government Exhibits 1, 2, 4, and 5 should be denied.

B. Search Warrant for Orme Street Residence (Gov't Ex. 3)

Wilson argues that the September 27, 2020 search warrant authorizing the search of the Orme Street Residence, Wilson's person, and the Pontiac Grand Am lacked probable cause because there is no information in the supporting affidavit that contraband would be found in these physical locations, only allegations that police found child pornography in the cloud on two Gmail accounts and a Microsoft OneDrive account linked to Wilson. (Dkt. 36 at 6-7.)

The Government counters that courts have long concluded that an agent's training and experience about how and where child pornography collectors keep their materials should be afforded deference, and therefore the issuing judge here appropriately relied on

SA Munkelwitz's assertions, based on his training and experience, that child pornography could be found in targeted locations. (Dkt. 37 at 12-13.) In addition, the Government argues that it is not unreasonable to believe that persons who trade and possess child pornography keep them in private spaces so as to not reveal their pedophilic tendencies to the outside world—such as a residence, person, or vehicle. (*Id.* at 13.)

The Eighth Circuit has "given substantial weight to testimony from qualified law enforcement agents about the extent to which pedophiles retain child pornography." *Lemon*, 590 F.3d at 615 (citing *United States v. Chrobak*, 289 F.3d 1043, 1046 (8th Cir. 2002)) (citations omitted); *see also United States v. Stults*, 575 F.3d 834, 844 (8th Cir. 2009) (finding probable cause based, in part, on an investigator's experience in child-pornography cases). Here, SA Munkelwitz provided the following information relating to his training and experience with respect to computer technology, child pornography and those who collect child pornography: that individuals who produce or collect child pornography using a computer or smartphone with Internet connection can store and distribute images quickly; large amounts of data can be stored on mobile telephones and mobile data storage devices no larger than a credit card; that it is common for individuals to keep devices like mobile telephones and data storage devices in their vehicles and on their persons due to their relatively small size and mobility; that individuals who have a sexual interest in children or who collect images of children will go to great lengths to conceal and protect their materials from discovery, theft, and damage; and that they often maintain their collections in a safe, secure and private environment such as within a

laptop computer, cell phone, or USB device, and maintain their collections on items stored in the privacy and security of their home or vehicle. (*See* Gov't Ex. 3 at 3-5.)

Moreover, it is important to emphasize that in reviewing whether there was probable cause to issue the warrant, the Court gives the issuing judge's determination "great deference,' examining the sufficiency of the supporting affidavit "using a 'common sense' and not a 'hypertechnical' approach." *United States v. Saddler*, 19 F.4th 1035, 1039 (8th Cir. 2021) (quoting *United States v. Grant*, 490 F.3d 627, 631-32 (8th Cir. 2007)). While Wilson focuses on the fact that the pornographic images included in the supporting affidavit were on servers outside of the Orme Residence and his vehicle, he ignores that the search warrant sufficiently connects him to the Orme Residence and to the vehicle, connects him to the two Gmail accounts and a Microsoft OneDrive account containing child pornography, links his cell phone to these accounts, and sets forth his status a registered sex offender. Therefore, there is a substantial basis to conclude that law enforcement had probable cause to search the Orme Street Residence and the Pontiac Grand Am because the affidavit showed that Wilson would likely have at least digital child pornography. Moreover, the expectation that Wilson would be viewing the child pornography at home is completely consistent with Eighth Circuit observations that child pornography crimes are generally carried out in the privacy of the home. *See Chrobak*, 289 F.3d at 1046 (holding a child-pornographer's email address, when linked to a suspect, provides probable cause to search the suspect's house); *see also United States v. Huyck*, 849 F.3d 432, 439-40 (8th Cir. 2017) (finding probable cause to search a suspect's house months after browsing a hard-to-access child-pornography website)

(quoting *Chrobak*, 289 F.3d at 1046); *United States v. Chase*, 717 F.3d 651, 653 (8th Cir. 2013) ("Chase argues specifically that the warrant failed to establish a nexus between the items to be seized—child pornography—and the location to be searched—Chase's residence. We reject this argument because '[t]he observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases.'") (quoting *United States v. Hyer*, 498 F. App'x 658, 660-61 (8th Cir. 2013), *cert. denied*, 134 S. Ct. 975 (2014); *United States v. McArthur*, 573 F.3d 608, 613-14 (8th Cir. 2009) (upholding probable cause to search a home computer where defendant found in personal possession of a single hard copy image of computer-modified child pornography, the defendant had multiple previous convictions, and affiant stated that images of child pornography are likely to be hoarded by persons interested in those materials and kept secret in secure places like a private residence). Similarly, given the evidence of the involvement with cell phones with the offending Google and Microsoft accounts, the connection of the phones to Wilson, their ability to connect wirelessly to the Internet and digital information (including digital pornography), and their inherently mobile nature, it is probable that such mobile devices containing evidence of child pornography could be found in Wilson's residence, on his person or in his vehicle.

Based on the totality of the circumstances, the Court finds that the September 27, 2020 Search Warrant is supported by sufficient probable cause and the Motion to Suppress should be denied.

C. *Leon* Exception

Because the Warrants were supported by probable cause (as set forth above), the Court need not determine whether the good-faith exception set forth in *United States v. Leon*, 468 U.S. 897 (1984), should apply. The Court finds, however, that even if the Warrants were lacking in probable cause, the officers' reliance on the Warrants would have been reasonable under *Leon*.

Under *Leon*, "'evidence seized pursuant to a search warrant issued by a [judge] that is later determined to be invalid[] will not be suppressed if the executing officer's reliance upon the warrant was objectively reasonable.'" *United States v. Houston*, 665 F.3d 991, 994 (8th Cir. 2012) (quoting *Proell*, 485 F.3d at 430). In *Leon*, the Supreme Court stated that "'searches pursuant to a warrant will rarely require any deep inquiry into reasonableness,' for 'a warrant issued by a magistrate [judge] normally suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" 468 U.S. at 922 (citations omitted). The *Leon* exception also applies to situations where information in a supporting affidavit is stale. *See Gettel*, 474 F.3d at 1086 ("Moreover, even assuming that the information in the affidavit was stale, the 'good faith' exception of [*Leon*] would apply.").

However, there are certain instances when "the purpose of the exclusionary rule—deterring police misconduct—will not be served by suppressing illegally seized evidence." *United States v. Martin*, 833 F.2d 752, 755 (8th Cir. 1987); *Leon*, 468 U.S. at 922-23. "When a police officer acts in an objectively reasonable manner in reliance on a subsequently invalidated search warrant, there is no rational reason for suppressing the

fruits of the search." *Martin*, 833 F.2d at 755. The Court's "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 923 n.23. The reviewing court should consider the totality of the circumstances, "including any information known to the officer but not included in the affidavit . . . ." *United States v. Jackson*, 784 F.3d 1227, 1231 (8th Cir. 2015) (citation omitted).

In this regard, evidence obtained as a result of an unconstitutional search should be suppressed under the following circumstances:

i. when the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge;

ii. when the issuing judge "wholly abandoned his judicial role" in issuing the warrant;

iii. when the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and

iv. when the warrant is "so facially deficient" that no police officer could reasonably presume the warrant to be valid.

Houston, 665 F.3d at 995 (quoting *Proell*, 485 F.3d at 431). "In determining the presence of good-faith reliance on a judge-issued search warrant, the court must consider [the] totality of circumstances, including information not presented to the judge issuing the warrant but known to the police officers." *United v. Clay*, 646 F.3d 1124, 1127 (8th Cir. 2011)). With respect to the third exception, the Eighth Circuit has explained: "'Entirely unreasonable' is not a phrase often used by the Supreme Court, and we find nothing in

Leon or in the Court's subsequent opinions that would justify our dilution of the Court's particularly strong choice of words." *Proell*, 485 F.3d at 432 (quoting *Carpenter,* 341 F.3d at 670).

Here, Wilson has not argued, nor does the Court find, that the affidavits were intentionally or recklessly misleading, or that the issuing judges wholly abandoned their judicial role in issuing the search warrants. As to the remaining exceptions, the Court has already concluded that the affidavits provided an adequate factual basis for the issuing judges to have found probable cause. Therefore, based on all the facts and circumstances of this case, it was not "entirely unreasonable" for law enforcement officers to rely on the Warrants.

* * *

In sum, for all of the reasons stated above, the Court recommends denial of Wilson's Motion to Suppress Evidence Obtained as a Result of Search and Seizure.

IV. RECOMMENDATION

Based on the files, records, and proceedings herein, **IT IS RECOMMENDED THAT:** Drayton Dean Wilson's Motion to Suppress Evidence Obtained as a Result of Search and Seizure (Dkt. 30) be **DENIED**.

DATED: March 9, 2022

s/Elizabeth Cowan Wright
ELIZABETH COWAN WRIGHT
United States Magistrate Judge

NOTICE

This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals.

Under District of Minnesota Local Rule 72.2(b)(1), "a party may file and serve specific written objections to a magistrate judge's proposed finding and recommendations within 14 days after being served a copy" of the Report and Recommendation. A party may respond to those objections within 14 days after being served a copy of the objections. D. Minn. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set for in D. Minn. LR 72.2(c).